Committee on
HOMELAND SECURITY
Chairman Michael McCaul

Opening Statement

March 20, 2013

Media Contacts: Mike Rosen, Charlotte Sellmyer

(202) 226-8417

Statement of Chairman Patrick Meehan (R-PA)
Subcommittee on Cybersecurity, Infrastructure Protection, and Security Technologies
Committee on Homeland Security

"Cyber Threats from China, Russia and Iran: Protecting American Critical Infrastructure"

March 20, 2013

Remarks as Prepared

I'd like to welcome everyone to today's hearing, which is our first Subcommittee hearing of the 113th Congress. This being our first hearing, I'm going to take care of a few housekeeping items right off the bat.

As some of you know, I chaired the Subcommittee on Counterterrorism and Intelligence last Congress. There are many overlapping issues in the cyber realm and I look forward to engaging in them over the next two years.

I'd like to begin by taking the opportunity to credit Ranking Member Clarke for her leadership on cybersecurity. You have been at this for a while and I look forward to working together in a bipartisan manner moving forward.

Second, I'd also like to take the opportunity to salute the former Chairman of this Subcommittee, Rep. Dan Lungren from California. Rep. Lungren served in Congress during the 1980s and after a stint at Attorney General of California in 1990s, felt compelled to serve again after September 11th. He was elected to the House again in 2004 and was involved in virtually every post-9/11

government policy response. His substance, knowledge, and exceptional legal acumen will be missed in this body. I wish him well and thank him for his service.

Finally, I'd like to welcome the new Members to the Subcommittee. In my experience, this Committee has operated in a bipartisan manner and I expect that to continue in the 113th Congress. I look forward to working with all of you.

Today's hearing is timely and relevant. We are examining the cyber threat posed by nation states: China, Russia, and Iran. I focus on the "nation state" aspect of this threat because it represents a new battlefield in state relations and we must prepare accordingly.

Since the New Year, there have been significant developments in the cyber domain, highlighted by the fact the U.S. Government has finally begun to name the nation states most responsible for cyber attacks against the United States. I believe identifying the threat is critical to combatting this problem and protecting our critical infrastructure.

Over the last two months, the Obama Administration has rightly placed cybersecurity at the top of the public agenda. In his State of the Union speech, President Obama specifically cited "foreign countries" swiping our corporate secrets, attacking our financial institutions, and sabotaging our power grid.

While he didn't name any specific countries, last week, Tom Donilon, the President's National Security Advisor, outed China as the place where cyber intrusions are emanating on "an unprecedented scale."

Also last week, in the Annual Threat Assessment by the U.S. Intelligence Community delivered to Congress last week, the Director of National Intelligence (DNI), James Clapper, named cyber as the top threat to U.S. national security. This represents a major shift in the threat assessment by the U.S. Intelligence Community and makes our work on this Committee even more important.

Lastly, *The New York Times* reported last week the President Obama discussed cybersecurity during a congratulatory phone call with the new Chinese President. The fact this issue is being addressed at the head-of-state level is an excellent development. I credit the Obama Administration for naming the threat and pushing for action.

With respect to identifying the threat, this Subcommittee has a history of identifying the threat and naming it publicly, often before it manifests itself. In fact, last year, former Rep. Lungren and I held a joint subcommittee hearing entitled, "The Iranian Cyber Threat to the Homeland" which identified Iran as a growing cyber threat.

Since that hearing, it has been widely reported that Iran conducted Distributed Denial of Service (DDoS) attacks against multiple American financial institutions. If true, I'd say that we were all

correct in our predictions last July. Both Mr. Cilluffo and Mr. Berman testified at that hearing and aptly predicted Iran's growing intent and capability to conduct a cyber attack against the U.S. homeland. I credit you both for your foresight on this issue when many underestimated the Iranian cyber threat.

I view today's hearing as a continuation of last year's hearing and I look forward to learning how the threat has evolved.

With respect to the Iranian cyber threat, I believe clarity is critically important. Iran is the world's largest state sponsor of terrorism and continues to pursue nuclear weapons to "wipe Israel off the map." In that sense, I believe we are dealing with a potentially irrational actor, which makes the Iranian cyber threat even more dangerous.

Common sense dictates that any regime willing to detonate a bomb at a Washington, D.C. restaurant to assassinate the Saudi Ambassador to the United States would surely be willing to conduct a major cyber attack against U.S. critical infrastructure. The U.S. government must make clear to the Iranians our "red lines" and make clear to them that if they escalate any cyber attacks against U.S. critical infrastructure, we will respond appropriately.

For the Iranians, cyber is just another tool through which to sow terror and repress its people. In the words of my good friend Michael Oren, Israeli Ambassador to the United States, Iran's main export is murder. It is important we all realize that, especially within the context of cyber.

To that ensure we have the clarity about the Iranian threat, I would like to enter into the record a February 16th op-ed in *The Wall Street Journal* by Ambassador Oren entitled "Iran's Global Business is Murder, Inc." The op-ed provides great detail on Iran's murderous regime. I have also asked staff to ensure a copy of the op-ed has been provided to Members at today's hearing and encourage you to read it closely.

In my view, we must assess the Iranian cyber threat through Ambassador Oren's perspective: "in the context of murder, bombings, kidnappings, and trade in drugs and guns." Their cyber attack capability is increasing and their intent is murderous. We must not forget it.

Without objection, so ordered.

Members are also lucky to have a representative from Mandiant Corp. here today to testify on the cyber threat posed by China. While I've already mentioned the Administration's naming of the Chinese threat, a great deal of credit goes to Mandiant for its long-term work identifying the specific Chinese military unit responsible for looting our intellectual property and technological innovations and publicly naming its actual geographic location. That report is a service to all policymakers trying to combat the Chinese cyber threat.

As the ultimate credit to Mandiant's report on China's cyber threat, I will quote perhaps the premier American intelligence official, former CIA and NSA Director and fellow Pennsylvanian, General Michael Hayden, who simply stated: "It was a wonderful report." General Hayden knows a thing or two about intelligence analysis so I view this as the ultimate validation of Mandiant's work.

With respect to the Russian cyber threat, I look forward to hearing from today's witnesses. Russia is often overlooked in the cyber threat realm, but they have the capability and have illustrated the intent to use it in Estonia and Georgia.

As our top traditional adversary in the game of espionage, I view cyberspace as a new, modern Cold War battlefield between the U.S. and Russia and we must prepare and respond appropriately.

While not the focus of today's hearing, I believe it is worth pointing out that North Korea has been the source of increased rhetoric pertaining to nuclear weapons and the Obama Administration has responded by announcing the addition of missile interceptors in Alaska over the next few years.

North Korea's cyber capability should not be underestimated and its intent is difficult to assess. It was widely reported North Korea conducted cyber attacks against South Korea and the United States in July 2009. We must keep a watchful eye on this continued threat actor.

As Chairman McCaul indicated at last week's full Committee hearing, the Committee plans to pass cybersecurity legislation in the coming weeks and months. We have been meeting with stakeholder groups affected by this issue and we encourage continued dialogue. The vast majority of critical infrastructure is owned by the private sector so there must be a true partnership between government and industry to ensure we are protected.

I look forward to continuing the conversation on these issues.

###